ZERO-TRUST CONTROLS

A CFO CHECKLIST FOR PROTECTING CASH, DATA, AND REPUTATION

Sharp CFO | WeDo CFO

Use this checklist to quickly assess whether your organization's access controls actually protect the business or just look good on paper.

---

1. Identity & Access Control

☐ **Every user has a unique login. No shared accounts. No exceptions.**
☐ **Multi-factor authentication (MFA) is required for all financial systems.**
☐ **Hardware-based MFA is required for:**

- **Banking platforms**
- **Payroll systems**
- **Tax filing software**

☐ **Access is reviewed quarterly by management, not just IT.**
☐ **Dormant accounts are automatically disabled after inactivity.**

Red Flag: Former employees, contractors, or vendors still have active credentials.

---

2. Least Privilege Enforcement

☐ **Users only have access to systems required for their role.**
☐ **Preparers cannot approve payments or change bank instructions.**
☐ **Reviewers cannot initiate transactions.**
☐ **Administrators cannot process or approve financial activity.**

☐ **Temporary access is time-limited and expires automatically.**

Red Flag: "Everyone needs access just in case."

---

3. Device Controls

☐ **Only approved, secured devices can access:**

We Do Books™ Scottsdale
15333 N Pima Rd, Suite 305
Scottsdale, AZ 85260
(855) 922-WeDo (9336)
wwwWeDoBooks.com

We Do Books™ Ventura County
1000 Town Center Dr, 300
Oxnard, CA 93036
(805) 389-7300
wwwWeDoBooks.com

We Do Books™ Wickenburg
581 W Wickenburg Way #C
Wickenburg, AZ 85390
(855) 735-1040
www.WDBwickenburg.com

- Accounting systems
- Payroll platforms
- Tax software
- Banking portals

☐ Devices are encrypted and centrally managed.
☐ Personal laptops are blocked from financial systems.
☐ Lost or stolen devices can be remotely disabled.

Red Flag: Finance staff logging in from personal or unknown devices.

---

4. Vendor & Contractor Access

☐ Vendors and contractors have separate access roles from employees.
☐ Vendor access is restricted to:

- Specific systems
- Specific data
- Specific time periods

☐ Vendor credentials automatically expire at the end of engagement.
☐ No vendor has access to banking or payment approval systems.

Red Flag: Vendors "borrowing" employee credentials to get work done.

---

5. Segregation of Duties (Technically Enforced)

☐ Payment initiation and approval are handled by different users.
☐ Bank detail changes require dual approval.
☐ Payroll changes require management approval outside the payroll team.
☐ System permissions enforce SoD. Policies alone do not count.

Red Flag: The system allows one person to override controls.

---

6. Monitoring & Alerts

☐ Alerts are enabled for:

- After-hours logins
- Foreign or unusual login locations

- Mass downloads or exports
- Changes to payment instructions

☐ Alerts are reviewed by management, not ignored in inboxes.
☐ Logs are retained for audit and forensic review.

Red Flag: "We have logs, but no one looks at them."

---

7. Backup & Recovery Readiness

☐ Financial data is backed up daily with immutable snapshots.
☐ Backups are stored offsite and cannot be overwritten by ransomware.
☐ Restore testing is performed at least annually.
☐ Access can be revoked immediately without disrupting operations.

Red Flag: Backups exist but have never been tested.

CFO Certification Question

If a regulator, insurer, or board member asked today:

"Can you confidently say unauthorized access would be detected and stopped?"

☐ Yes
☐ No
☐ I hope so (not acceptable)

The Sharp CFO Bottom Line

Zero-trust is not an IT framework.
It is a financial control discipline.

If access is permanent, exposure is guaranteed.
If controls aren't enforced by systems, they don't exist.
And if no one owns oversight, losses will eventually surface.

At Sharp CFO / WeDo CFO, we evaluate zero-trust the same way we evaluate cash controls and risk exposure: practically, skeptically, and with the assumption that something will eventually go wrong.

Because that's how businesses actually fail.

Score Yourself

Zero-Trust Readiness for Finance Teams

Sharp CFO | WeDo CFO

For each item below, score your organization honestly. This is not a compliance exercise. This is a risk exposure exercise.

- **2 points** = Fully implemented and enforced
- **1 point** = Partially implemented or inconsistently enforced
- **0 points** = Not implemented or "planned"

---

1. Identity & Access (0–10 points)

☐ Unique user accounts for all staff, contractors, and vendors
☐ MFA required for all financial systems
☐ Hardware MFA for banking, payroll, and tax platforms
☐ Quarterly access reviews performed by management
☐ Automatic disablement of inactive accounts

Subtotal: ___ / 10

---

2. Least Privilege (0–10 points)

☐ Role-based access tied to job function
☐ No blanket or "just in case" permissions
☐ Temporary access expires automatically
☐ Privileged access reviewed regularly
☐ Access changes documented and approved

Subtotal: ___ / 10

---

3. Device Controls (0–10 points)

☐ Only approved devices can access finance systems
☐ Devices are encrypted and centrally managed
☐ Personal laptops blocked from financial platforms
☐ Remote wipe enabled for lost or stolen devices
☐ Device compliance checked at each login

Subtotal: ___ / 10

---

4. Vendor & Contractor Access (0–10 points)

☐ Vendors use separate accounts from employees
☐ Vendor access limited to required systems only
☐ Access automatically expires at engagement end
☐ No vendor access to banking or payment approval
☐ Vendor access reviewed post-engagement

Subtotal: ___ / 10

---

5. Segregation of Duties (0–10 points)

☐ Initiation and approval are technically enforced
☐ Dual approval required for payment changes
☐ Payroll changes require independent approval
☐ No single user can override controls
☐ Exceptions require documented authorization

Subtotal: ___ / 10

---

6. Monitoring & Alerts (0–10 points)

☐ Alerts for after-hours or unusual logins
☐ Alerts for mass downloads or exports
☐ Alerts for payment or bank detail changes
☐ Alerts reviewed by management
☐ Logs retained and accessible for review

Subtotal: ___ / 10

---

7. Backup & Recovery (0–10 points)

☐ Daily backups of all financial data
☐ Immutable snapshots enabled
☐ Offsite or offline backup storage
☐ Restore testing performed annually
☐ Immediate access revocation capability

Subtotal: ___ / 10

Total Score: ___ / 70

What Your Score Means

60–70: Controlled
You've treated zero-trust like a financial discipline. Risk still exists, but it's managed.

45–59: Exposed
Controls exist, but enforcement is inconsistent. This is where most real-world losses occur.

Below 45: Vulnerable
Access is too broad, oversight is weak, and fraud or data loss is a matter of timing.

No judgment. Just math.

The Sharp CFO Bottom Line

Zero-trust isn't about perfection.
It's about reducing the number of ways something can quietly go wrong.

At **Sharp CFO** / **WeDo CFO**, we use this scorecard the same way we use cash-flow forecasts and internal control reviews. It tells us where risk actually lives, not where policy says it shouldn't.

If your score makes you uncomfortable, that's the point.
Discomfort is cheaper than remediation.